*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**DATE(S) ISSUED:**
1/13/2010

**SUBJECT:**
Vulnerabilities in Adobe Reader and Adobe Acrobat Could Allow For Remote Code Execution

**OVERVIEW:**
Multiple vulnerabilities discovered in the Adobe Acrobat and Adobe Reader applications could allow attackers to execute arbitrary code on affected systems. Adobe Reader allows users to view Portable Document Format (PDF) files. Adobe Acrobat offers users additional features such as the ability to create PDF files. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

**SYSTEMS AFFECTED:**

Adobe Acrobat Professional 9.2 and prior
Adobe Acrobat Professional 8.1.7 and prior
Adobe Acrobat Standard 9.2 and prior
Adobe Acrobat Standard 8.1.7 and prior
Adobe Reader 9.2 and prior
Adobe Reader 8.1.7 and prior

**RISK:**

**Government:**
Large and medium government entities: **High**
Small government entities: **High**

**Businesses:**
Large and medium business entities: **High**
Small business entities: **High**

**Home users: High**

**DESCRIPTION:**
Eight security vulnerabilities have been identified in Adobe Reader and Adobe Acrobat. These vulnerabilities can be exploited if a user opens a malicious file designed to trigger these issues.  The vulnerabilities are as follows:

A use-after-free vulnerability in Multimedia.api that could lead to code execution.
A vulnerability involving an array boundary condition error in U3D support that could lead to code execution.
A vulnerability involving a DLL-loading issue in 3D that could allow arbitrary code execution.
A memory corruption vulnerability related to processing a 'JPC_MS_RGN'  marker in the Jp2c stream of a JpxDecode encoded data stream that could lead to code execution.
A vulnerability involving a script injection error by changing the Enhanced Security default.
A vulnerability involving a null-pointer dereference error that could lead to denial of service.

A vulnerability involving a buffer overflow in the Download Manager that could lead to code execution.
A vulnerability involving an integer overflow vulnerability in U3D support that could lead to code execution.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user for seven of the eight vulnerabilities. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

**RECOMMENDATIONS:**
The following actions should be taken:

- Apply appropriate updates provided by Adobe to vulnerable systems immediately after appropriate testing.
- Systems running Adobe Reader 9.2 and Acrobat 9.2 and earlier versions should update to Adobe Reader 9.3 and Acrobat 9.3.
- Systems running Adobe Acrobat 8.1.7 and earlier versions should update to Acrobat 8.2.
- Do not open email attachments from unknown or un-trusted sources.
- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

**REFERENCES:**

**Adobe:**
http://www.adobe.com/support/security/bulletins/apsb10-02.html

**Security Focus:**
http://www.securityfocus.com/bid/37753
http://www.securityfocus.com/bid/37756
http://www.securityfocus.com/bid/37757
http://www.securityfocus.com/bid/37758
http://www.securityfocus.com/bid/37759
http://www.securityfocus.com/bid/37760
http://www.securityfocus.com/bid/37761
http://www.securityfocus.com/bid/37763

**Secunia:**
http://secunia.com/advisories/37690/

**CVE:**
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3953
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3954
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3955
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3956
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3957
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3958
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3959
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4324